UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

UNITED STATES OF AMERICA	§	
	§	**Criminal No. 24-CR-00298**
V.	§	
	§	
EITHAN HAIM	§	

DEFENDANT'S RENEWED MOTION TO DISMISS

The defendant, Dr. Eithan Haim, renews his motion for the Court to dismiss the (second) superseding indictment and the case with prejudice.

Despite protestations to the contrary at the November 15 hearing, the government has dropped any reference by which the Privacy Rule could be incorporated. The second superseding indictment, Dkt. No. 110, now charges solely that Dr. Haim obtained individually identifiable health information (IIHI) "without authorization" for all counts.

While the case was already in uncharted territory, that much is now beyond dispute. It appears that the government has never tried a HIPAA case solely on a "without authorization" theory, and it has certainly never abandoned the Privacy Rule to get there. No case has examined what "without authorization" means in HIPAA. So the Court will have to make an unprecedented legal choice one way or the other, either to follow the Supreme Court's guidance in *Van Buren* or throw the

question to the jury while dealing with the many legal and factual difficulties that necessarily follow, including through future motions in limine.

Given the thoroughness of the defense's briefing of the issues in its earlier motion to dismiss, Dkt. No. 91, and its reply in support of that, Dkt. No. 96, this renewed motion will address only a few points raised at the November 15 hearing and summarize the key points made in the briefs. As explained in the motion to dismiss, there is no dispute that the hospital granted Dr. Haim access to its electronic medical records system, Mot. at 15–16, so if "without authorization" is a categorical "gates-up-or-down inquiry" there is no point in maintaining this prosecution.

ARGUMENT

I. Nothing discussed at the November 15 hearing changes the analysis.

The government has not attempted to comprehensively rebut the arguments on why "without authorization" must be limited as in *Van Buren*. It has responded only piecemeal. At the November 15 hearing, it addressed one point regarding the interpretation of the HIPAA text and one point regarding interaction with the Privacy Rule. Neither of these points moves the needle.

On the text, the defense has explained at length why "without authorization" should be read in the same manner as the same phrase in the Computer Fraud and Abuse Act (CFAA). Under that reading, authorization to obtain IIHI in some circumstances means such an act is not "without authorization" in others. Whether

framed as a "gates-up-or-down inquiry" or analogized to pregnancy, there is no such thing as a little authorization. This reading makes perfect sense given that the more fine-grained Privacy Rule, modified over time by HHS and Congress, was meant to govern anyone with any authorization.

The government's textual response has been that the meaning of "without authorization" in the CFAA cannot inform the meaning of the same phrase in HIPAA because they are focused on different criminal acts. Dkt. No. 93 at 6–7. According to the government, HIPAA criminalizes obtaining information, while the CFAA criminalizes the means of obtaining information, so the same words in both share no content. At the hearing, the government stated: "The *actus reus*, as outlined in the CFAA, is how you access the computer system, which is completely different than what HIPAA was focused on." Tr. at 47–48.

Whether phrased in Latin or not, the argument has no force. The parallel between the statutory texts is obvious. Each punishes someone who:

- "accesses a computer without authorization . . . and thereby obtains . . . information" (CFAA), or
- "obtained . . . such information without authorization" (HIPAA).

The structure is the same: verb, object, adverbial phrase ("without authorization"). As the defense explained at the hearing, Tr. at 43–44, the verbs are different because

at the time of HIPAA's passage, almost all patient records were on paper.[1] Yet the purpose of both statutory provisions is the same—protecting information. And the adverbial phrase "without authorization" functions in the same manner and has the same meaning.

While the government argues that "accesses" in the CFAA serves as the means of committing the offense, that is incorrect. The conduct prohibited is accessing without authorization; that is the offensive act. The CFAA adds obtaining information as the required result because that is the injury. In HIPAA, those two are combined into the same act. Again, the actual manner of committing the crime—without authorization—functions the same way.

Beyond the text, the defense also asserts that the government's abandonment of the Privacy Rule creates insurmountable difficulties for using "without authorization" to turn the hospital's policies on electronic access into criminal prohibitions. It would be absurd if the government, though unable to directly hold Dr. Haim criminally liable for the use-based prohibitions in the Privacy Rule, can punish him simply because the hospital incorporates those same prohibitions into its own policies. The government's answer at the hearing was that "[O]f course hospitals are bound by the Privacy Rule. They're bound by the regulations. If

[1] One purpose of HIPAA and the later HITECH Act (which added the "without authorization" clause) was to encourage the adoption and standardization of electronic medical records systems. *See, e.g.*, Cong. Research Serv., The Health Information Technology for Economic and Clinical Health (HITECH) Act (Apr. 27, 2009), https://crsreports.congress.gov/product/pdf/R/R40161/9.

hospitals don't follow the regulations, they are then subject to civil liability under the regulations." Tr. at 36. To lay this issue to rest, the government is wrong. Its argument was premised on the assertion that the government was not "abandoning the Privacy Rule," *id.*, which the defense refuted at the hearing by quoting the government's own brief, *id.* at 32 (quoting Dkt. No. 93 at 12). The government has effectively conceded the issue by dropping any way to incorporate the Privacy Rule into the second superseding indictment.[2]

But this key point remains: a necessary corollary of the defense's statutory and constitutional arguments against the Privacy Rule is that it binds no one, not even the hospital. *See* Mot. at 21–24. So the government cannot use the back door of hospital policies premised on the enforceability of the Privacy Rule to punish Dr. Haim. Even so, if "without authorization" becomes a pure question of fact incorporating hospital policies, then Dr. Haim must still be able to rely on any uses permitted by the Privacy Rule as a shield, even though the government cannot rely upon Privacy Rule-based policies as a sword. That will necessarily require briefing the issue through a motion in limine to ensure that the government does not present prejudicial evidence.

[2] It is the government's abandonment of the Privacy Rule that leads to the result the government protested at the hearing, where "any person working in a hospital can go look up anybody's medical file under any circumstance they want, for whatever reason they want, and it's okay." Tr. at 28. The "cases after cases" the government referenced, *id.*, are ones that proceeded assuming the validity of the Privacy Rule or where the defendant pleaded guilty. At the same time, the states, including Texas, have their own medical privacy laws that will still govern physicians.

II. The government has not rebutted the arguments about the limited nature of "without authorization."

The defense presented a full suite of arguments demonstrating the limited nature of "without authorization." It recites a summary here.

On the text:

- As discussed above, the relevant HIPAA and CFAA provisions are in parallel form, so the same phrase should be interpreted the same way in both.

- HIPAA lacks the "exceeds authorized access" companion crime from the CFAA, and even that broader crime still does not encompass "'using' a computer network in a way contrary to 'what your job or policy prohibits'" or for an "improper purpose," *Van Buren v. United States*, 593 U.S. 374, 390 (2021). So "without authorization" in HIPAA does not criminalize obtaining information contrary to hospital policy. Mot. at 11–12.

- The Solicitor General[3] and the petitioner in *Van Buren* agreed that "without authorization" is a "gates-up-or-down inquiry," Mot. at 12, and this was not mere dicta (as the government asserted at the hearing, Tr. at 47) because the Supreme Court relied on this concession, *see Van Buren*, 593 U.S. at 391.

On the legislative history:

- Congress added the "without authorization" clause to encompass those people *not* considered "covered entities" under HIPAA because the Department of Justice Office of Legal Counsel determined that only "covered entities" could be criminally liable. Mot. at 13. Doctors granted access would ordinarily be "covered entities."

On policy and judicial administrability considerations:

- Allowing "without authorization" to incorporate hospital policies would raise "intensely factual questions" that "will be matched by the excruciatingly specific evidence" necessary at trial, such as who can amend those policies and how they apply in specific circumstances. Mot. at 15.

[3] Petitioner's counsel in *Van Buren* now serves as the Principal Deputy Solicitor General.

On the interaction with the Privacy Rule:

- Even if the Privacy Rule were effectual, it would make little sense for the "without authorization" clause to overlap with the Privacy Rule substantially, creating surplusage. Reply at 9. The clause was never meant to regulate doctors with access to medical records.

- If "without authorization" incorporates whatever policies a hospital has, then the hospital could impose arbitrary criminal liability or even prohibit uses or disclosures permitted by the Privacy Rule, including to law enforcement or for preventing serious and imminent threats to health. Reply at 10–11.

On the constitutional problems:

- Adopting the government's view of "without authorization" creates intertwined notice and vagueness problems in two ways: it is unclear in advance what "without authorization" means and what liability the hospital will impose with whatever rules it creates. Many courts noted these same problems in the context of the CFAA. Reply at 11–13.

- Under the government's view, the notice problem in HIPAA is even worse than it was for the CFAA because the government believes there is no *mens rea* required—a doctor need no notice of the hospital's policies to be held criminally liable for violating them. Reply at 13–14.

- Allowing a private party (the hospital) to set rules under which any violation is criminally punished represents an unconstitutional delegation of authority. Reply at 14–15.

On the canons of construction:

- Given the constitutional problems with the government's view of "without authorization," the defense's position must be adopted under the canon of constitutional avoidance if it is permissible, and *Van Buren* proves that it is. Reply at 15.

- Even if all this analysis left doubts, "without authorization" would at best be grievously ambiguous, and the rule of lenity would likewise favor the defense's interpretation. *Id.*

CONCLUSION

The Court should determine that "without authorization" is a "gates-up-or-down inquiry" and dismiss the case with prejudice.

Dated: November 27, 2024

Respectfully submitted,

Ryan Patrick
Attorney-in-Charge
TX State Bar 24049274
SDTX No. 3006419
Haynes and Boone LLP
1221 McKinney Street, Suite 4000
Houston, Texas 77010
Tel: 713.547.2000
Fax: 713.547.2600
ryan.patrick@haynesboone.com

Mark D. Lytle
DC Bar 1765392
SDTX No. 3884197
Nixon Peabody LLP
799 9th Street NW, Suite 500
Washington, D.C. 20001
Tel: 202.585.8435
Fax: 202.585.8080
mlytle@nixonpeabody.com

Marcella C. Burke
TX State Bar 24080734
SDTX No. 1692341
Burke Law Group, PLLC
1000 Main St., Suite 2300
Houston, TX 77002
Tel: 832.987.2214
Fax: 832.793.0045
marcella@burkegroup.law

/s/ *Jeffrey A. Hall*
Jeffrey A. Hall
VA State Bar 82175
SDTX No. 3885025
Burke Law Group, PLLC
2001 L. Street N.W., Suite 500
Washington, D.C. 20036
Tel: 832.968.7564
Fax: 832.793.0045
jeff@burkegroup.law

ATTORNEYS FOR DEFENDANT EITHAN DAVID HAIM

CERTIFICATE OF SERVICE

The undersigned attorney hereby certifies that a true and correct copy of the above and foregoing document has been filed and served on November 27, 2024 using the CM/ECF system, which will send notification of such filing to all counsel of record.

/s/ *Jeffrey A. Hall*
Jeffrey A. Hall